DK•CERT

Trendrapport

It-sikkerhed i første kvartal 2010

DANMARKS IT-CENTER FOR
UDDANNELSE OG FORSKNING

UNI•C

Redaktion: Shehzad Ahmad, Jens Borup Pedersen, DK•CERT

Grafisk arbejde: Kirsten Tobine Hougaard, UNI•C

Foto: colourbox.com

DK•CERT

Det er DK•CERTs mission at skabe øget fokus på it-sikkerhed ved at opbygge og skabe aktuel, relevant og brugbar viden. Denne viden gør DK•CERT i stand til at offentliggøre og udsende advarsler og anden information om potentielle risici og begyndende sikkerhedsproblemer.

DK•CERT bygger på en vision om at skabe samfundsmæssig værdi i form af øget it-sikkerhed. Det sker gennem offentliggørelse af viden om it-sikkerhed skabt gennem samarbejde med den offentlige og private sektor, forsknings- og undervisningsverdenen, samt internationale samarbejdspartnere.

Denne viden benytter DK•CERT til at udvikle services, der skaber merværdi for DK•CERTs kunder og øvrige interessenter og sætter dem i stand til bedre at sikre deres it-systemer.

DK•CERT, det danske Computer Emergency Response Team, blev oprettet i 1991 som en afdeling af UNI•C, Danmarks it-center for uddannelse og forskning, der er en styrelse under Undervisningsministeriet.

DK•CERT var blandt pionererne, der først i 1990'erne tog initiativ til etablering af et internationalt samarbejde om it-sikkerhed med grundidé i CERT/- CC i USA. Som led i dette samarbejde overvåger, rådgiver og informerer DK•CERT om it-sikkerhed i Danmark.

Indholdsfortegnelse

1. Resume

Som året forinden bød januar måned 2010 på mange anmeldelser om sikkerhedshændelser til DK•CERT, efterfulgt af nogle mere stille måneder. Generelt synes antallet at have stabiliseret sig efter nogle års fald.

En væsentlig tendens for første kvartal 2010 er, at der i stigende grad scannes efter allerede installerede programmer til fjernadministration af den scannede computer, snarere end sårbare programmer. Således var mere end 50% af alle scanninger efter porte, der benyttes af programmer til fjernadministration.

Trojanske heste er stadig den mest populær *malware*-type. *Vira* og netværksbaserede *orme* er på retur til fordel for *malware*, der ikke selv besidder evnen til at sprede sig. Derimod er sårbare legale webservere blevet en central del af forsyningskæden for spredning af *malware*. DK•CERT modtog således i første kvartal af 2009 et stigende antal anmeldelser vedrørende *trojanske heste* og *phishing*-sider placeret på danske webservere.

Offentliggørelserne af de *sårbarheder*, der udstyres med et *CVE-nummer*, bliver stadig færre i antal. Således blev der i første kvartal af 2010 offentliggjort 1.140 nye *CVE-nummererede sårbarheder*, hvoraf cirka en tredjedel kan relateres til standard webapplikationer. Generelt findes der *sårbarheder* i alle programmer og ingen hverken produkter eller producenter er sikre.

De kriminelle grupperinger er i dag professionelle i både mål og midler. Det afspejles ved angrebet mod PBS. Vi tror desværre, at denne udvikling fortsætter, således at vi som borgere og organisationer udsættes for mere målrettede og sofistikerede angreb tilpasset fx geografi og aktuelle begivenheder. Det understreges af måden hvorpå jordskælvskatastrofen i Haiti blev udnyttet, samt en langsom optrapning af internetkriminalitet, der kan relateres til sommerens verdensmesterskab i fodbold. It-kriminalitet er nemlig en god forretning for organiserede kriminelle grupperinger.

Heldigvis står vi ikke forsvarsløse tilbage. Internationalt har der været en stigende vilje og evne til at stoppe internetaktiviteter, der er i strid med loven. Tilsvarende tror vi herhjemme, at etableringen af GovCERT til et bredere publikum end staten vil gavne den danske it-sikkerhed, der ikke kan isoleres til brancher og sektorer. Når man i staten begynder implementeringen af *ISO 27001*, bør de refleksioner som dette arbejde medfører, tilsvarende give grobund for optimisme for it-sikkerheden i fremtidens Danmark.

Det er vores håb, at du kan bruge informationerne på de følgende sider som inspiration, således at vi kan være med til at sikre de danske it-aktiver.

2. Første kvartal 2010 i tal

Du præsenteres i dette afsnit for tal og statistikker fra første kvartal 2010, der fortæller en historie om it-kriminalitetens udvikling i løbet af årets første tre måneder. Data er primært udtrukket fra vores egne systemer, og dækker hovedsagelig *Forskningsnettet* samt enkelte andre netværk, som DK•CERT overvåger. Enkelte tal er suppleret og perspektiveret med data fra internettets åbne kilder.

Afsnittet har fokus på de sikkerhedshændelser, der i løbet af perioden er blevet anmeldt til DK•CERT. En væsentlig del omhandler scanninger mod tilgængelige systemer på internettet, der beskrives særskilt. Derudover beskrives tal vedrørende malware og andet uønsket materiale, der florerer på internettet. Afsnittet afsluttes med statistikker vedrørende årets nye *sårbarheder* samt de *sårbarheder*, vi har kunnet konstatere ved scanninger af vores kunders systemer.

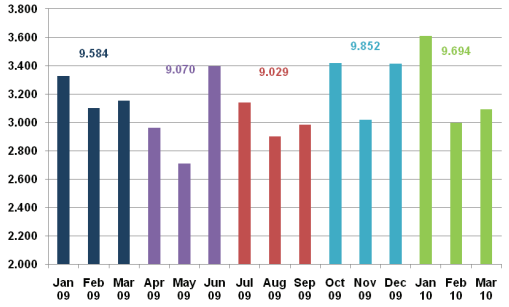
2.1 Sikkerhedshændelser i første kvartal 2010

Antallet af sikkerhedshændelser anmeldt til DK•CERT, har gennem de seneste 15 måneder varieret meget (Figur 1). De første tre kvartaler af 2009 viste på trods af meget store månedlige variationer en svagt faldende tendens i antallet af anmeldte sikkerhedshændelser. Siden er dette igen steget, således at der i første kvartal af 2010 blev anmeldt tilnærmelsesvis samme antal sikkerhedshændelser som i første kvartal af 2009. En væsentligste årsag er, at systemscanninger anmeldt til DK•CERT har fulgt stort set samme tendens. Således udgjorde anmeldelse om scanninger af vores kunders it-systemer i første kvartal af 2010 8.683, eller næsten 90% af alle anmeldelser.

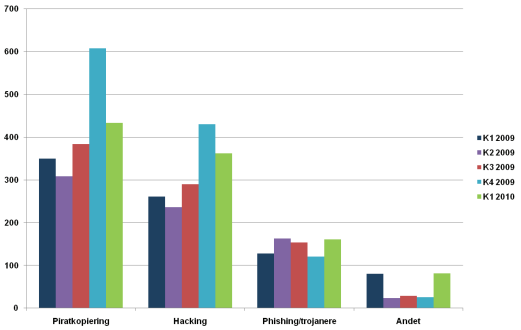
På trods af et fald i anmeldelser af hacking og piratkopiering fra fjerde kvartal 2009 til første kvartal 2010 er der over de seneste 15 måneder sket en stigning i anmeldelserne af disse hændelsestyper (Figur 2). Tilsvarende er mængden af sager om *phishing*- og *trojansk hest*-inficerede websites steget efter et fald i fjerde kvartal 2009. I modsætning de øvrige hændelseskategorier er kategorien "Hacking" i denne sammenhæng ikke helt entydig. Den dækker både over vellykkede systemkompromitteringer såvel som i enkelte tilfælde mistanke om og forsøg på kompromittering.

2.2 Scanninger

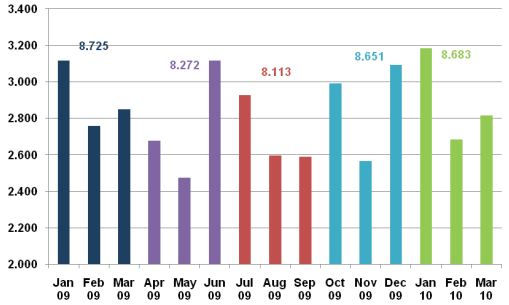
DK•CERT modtog i første kvartal af 2010 8.683 anmeldelser om scanninger efter svarende og sårbare services på internettet, hvilket er på samme niveau som et år tidligere (Figur 3). Tilsvarende har antallet af angribende IP-adresser som i 2009 været på ca. 1.500 nye adresser pr. måned, eller i alt 4.522 forskellige IP-adresser. Ligesom i første kvartal af 2009 modtog vi flest scanninger i januar måned, hvorefter aktiviteten faldt i februar for herefter at stige svagt i marts.



Figur 1. Sikkerhedshændelser anmeldt til DK•CERT.



Figur 2. Væsentligste hændelsestyper anmeldt til DK•CERT 2010.



Figur 3. Scanninger anmeldt til DK•CERT.

2010 adskiller sig primært ved antallet af forskellige porte og protokoller, der blev scannet efter. Der blev i første kvartal af 2010 anmeldt scanninger mod 254 forskellige porte. Således blev der i første kvartal af 2010 anmeldt scanninger mod et bredere spekter af porte og protokoller end i hele 2009, hvor der kun blev scannet efter 152 forskellige porte og protokoller. Dette afspejler sig også ved, at ICMP-ping af store netsegmenter kun indgik i 20,7% af scanningerne (Figur 4), mod 30,8% i hele 2009. Ping er som sådan legal trafik og bør isoleret set ikke give anledning til større postyr. Når det i disse tilfælde alligevel har givet anledning til, at ping blev anmeldt til DK•CERT, skyldes det mængden af trafik snare end arten.

Mest bemærkelsesværdigt var det, at omkring 50% af alle scanninger i første kvartal 2010 var på porte, der bl.a. benyttes af services som bruges til fjernstyring af computere. Både TCP-portene 1024, 4899 og 5900 benyttes af legale programmer til fjernadministration, mens port 3072 blandt andet (mis)bruges af et kendt *botnet*-program (Figur 4). Tilsvarende dækker en stor del af de angrebene på TCP-port 22 (ssh) over *brute-force* angreb, hvor der forsøges login ved at "gætte" kombinationer af brugernavne og passwords. Det tyder således på, at der ikke længere blindt afdækkes sårbarheder ved scanninger, men man i højere grad forsøger at tilgå allerede kompromitterede systemer eller systemer, der er "lettere" at kompromittere.

Scanninger mod HTTP og HTTPS på henholdsvis TCP-port 80 og 443 var heller ikke i første kvartal af 2010 blandt de hyppigst anmeldte, da de ofte ikke opdages eller registreres som forsøg på kompromittering. For at undersøge om en webserver er sårbar, behøves således kun ganske få opslag på Google, og hverken mængden eller typen af disse forespørgsler giver normalt anledning til mistænksomhed.

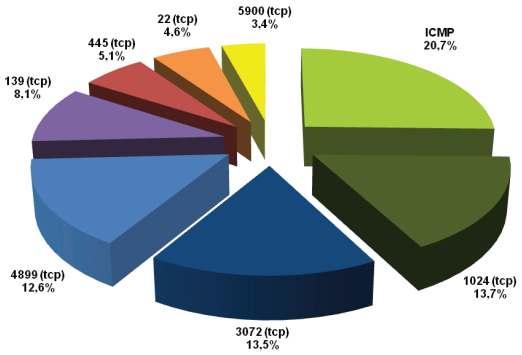
Hovedparten af de scanninger, som i første kvartal af 2010 blev anmeldt til DK•CERT, blev foretaget fra IP-adresser tilhørende ISP'er i USA (Figur 5). I forhold til 2009 har man i både Tyrkiet og Rusland været mere aktive i samme periode, mens aktiviteten fra Kina er faldet til næsten det halve. Danmark endte med 1,2% af alle anmeldelser om scanning på en 18. plads i førstekvartal 2010.

2.3 Malware m.m.

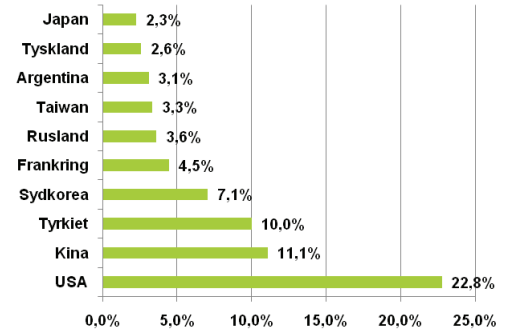
2010 har indtil nu ikke budt på væsentlige udbrud af hverken nye vira eller netværksbaserede *orme*. I forhold til 2009 er der sket et fald i inficeringer med *orme* og vira i Danmark, der sidste år stod for sammenlagt 9% af alle danske *malware*-inficeringer. Den hyppigst fjernede *malware* i Danmark var også i første kvartal af 2010 *trojanske heste* (Figur 6). Dette understreger Gartners ord:

"*Malware distribution methods have shifted from traditional viruses, mass mailers and network worms to Web-hosted attacks*[1]."

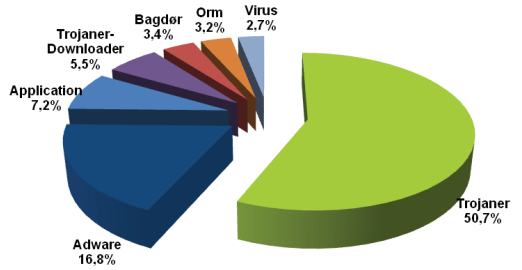
Således har der været et konstant eller svagt stigende antal *trojanske heste* og *phishing*-sider hostet på danske servere. Efter et dyk sidst i 2009 blev der igen i første kvartal af 2010 anmeldt flere danske websites, der hostede *malware* (Figur



Figur 4. Hyppigst scannede portnumre i første kvartal 2010.



Figur 5. Scannende IP-adressers landetilhørsforhold i første kvartal 2010.



Figur 6. Hyppigste danske malware-infektioner identificeret af F-Secure i 2010[2].

1 *Gartner, 2008, "Why malware filtering is necessary in the web gateway".*

2 *F-secure.com, 2009; "F-Secure security lab - virus world map".*

7). Langt størstedelen af disse formodes at være kompromitterede legale websites, der i 2009 stod for hosting af cirka 80% af al webhostet *malware*[3]. En stigende andel kan formodes i fremtiden at blive hostet i *botnet*, der benytter *fast-flux* teknologi, hvorved levetiden mangedobles[4].

2.4. Sårbarheder

Der blev i første kvartal af 2010 offentliggjort 1.140 *CVE-nummererede* sårbarheder i standardprogrammer, hvilket synes at fortsætte en faldende tendens (Figur 8).

Mens der tidligere blev fundet og offentliggjort flest *sårbarheder* i operativsystemet, er det nu applikationer, der kører oven på operativsystemet, som er i overtal[7]. Således udgjorde sårbarheder, der typisk findes i webapplikationer, mere end en tredjedel af alle nye *CVE-nummererede sårbarheder*, som blev offentliggjort i første kvartal 2010 (Figur 9). I tillæg hertil kommer *sårbarheder* i den specifikke implementering af en webapplikation, der ikke offentliggøres med et *CVE-nummer*.

Listen over de programmer hvortil der blev offentliggjort flest *CVE-nummererede sårbarheder*, domineres stadig af de store operativsystemer fra blandt andre Apple og Microsoft (Figur 10). Derudover er internetbrowsere fra både Microsoft, Apple, Mozilla og Google repræsenteret.

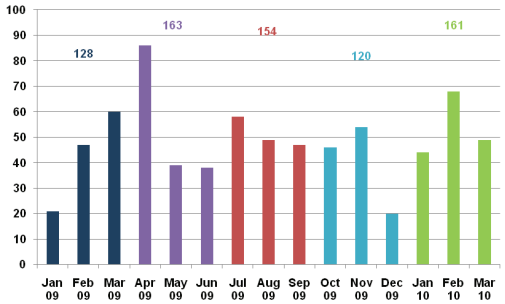
DK•CERT foretog i første kvartal af 2010 *sårbarhedsscanning* af cirka 10.000 forskellige IP-adresser, hovedsagelig placeret på *Forskningsnettet*. Af disse svarede små 5%. I alt ca. 3% havde i gennemsnit fire *CVE-nummererede sårbarheder*. De øvrige IP-adresser må formodes ikke at være i brug eller være beskyttet bag en firewall.

Der blev ved scanningerne konstateret *sårbarheder* på 21 forskellige porte og/eller protokoller. Flest sårbarheder blev der konstateret på TCP-port 80 og 443, der benyttes af webapplikationer (Figur 11). Applikationsspecifikke *sårbarheder* forårsaget af fx mangelfuld inputvalidering på webapplikationer fremgår ikke af statistikken, da de kun sjældent offentliggøres med et *CVE-nummer*.

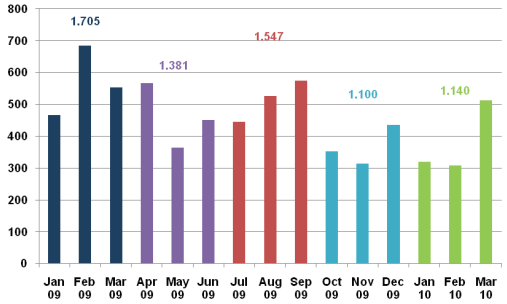
Malware

"Malware er en sammentrækning af de engelske ord malicious software (på dansk: 'ondsindet programkode'). Det bruges som en fællesbetegnelse for en række kategorier af computerprogrammer, der gør skadelige eller uønskede ting på de computere, de kører på[5]."

Malware kan opdeles i en række kategorier, som fx vira, orme, trojanske heste, keyloggere, spyware, adware,scareware, botnet-programmer og lignende.



Figur 7: Websites med trojanske heste og phishing-sider anmeldt til DK•CERT.



Figur 8. Offentliggjorte CVE-nummererede sårbarheder[6].

3 *MessageLabs Intelligence, 2009; "Messagelabs intelligence Q3/september 2009".*

4 *Havard.edu, 2009; "The economics of online crime".*

5 *Wikipedia.org, 2009; "Malware".*

6 *nvd.nist.gov; "CVE and CCE statistics query page".*

7 *Sans.org, 2009; "The top cyber security risks".*

3. Overskrifter fra første kvartal 2010

I dette afsnit beskrives en række af de overskrifter fra første kvartal 2010, som har været væsentlige fra vores perspektiv i den danske del af it-sikkerhedsbranchen. Der er ingen umiddelbar sammenhæng mellem de enkeltstående begivenheder, som dog tegner et billede af både it-kriminaliteten og de modforholdsregler, der foretages nationalt såvel som internationalt.

3.1. Jordskælvet i Haiti

Jordskælvskatastrofen, der den 12. januar 2010 ramte Haiti, medførte både herhjemme og i udlandet forsøg på at udnytte katastrofen til egen økonomisk vinding. Flere steder oplevede man herhjemme falske indsamlere, der udgav sig for at komme fra Dansk Røde Kors, Red Barnet og lignende organisationer. Også på internettet florerede de falske indsamlinger bakket op af mailkampagner, der opfordrede til at støtte redningsarbejdet i Haiti.

Derudover udnyttede de it-kriminelle søgemaskineoptimering til at eksponere falske indsamlinger og *skadelig kode* for brugere, der søgte informationer om katastrofen. Målet med disse systematiske kampagner var bl.a. at lokke brugere til at besøge særligt indrettede websider, der tilbød *skadelig kode* i form af falske sikkerhedsprogrammer, *trojanske heste* og lignende.

3.2. ISO 27001, "ny" standard for it-sikkerhed i staten

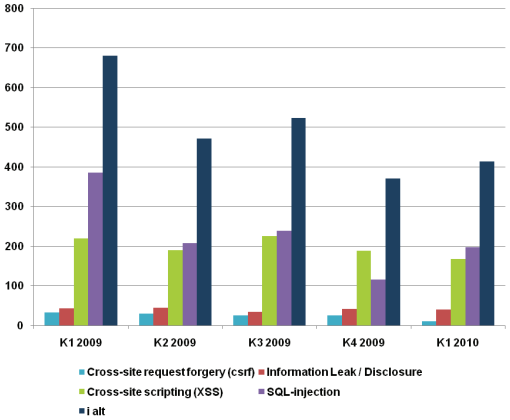
I februar 2010 besluttede den danske regering, at de statslige institutioner skulle overgå til den internationale sikkerhedsstandard, *ISO 27001*, i stedet for *DS 484*, der har været benyttet siden 2007. Det sker som led i regeringens handlingsplan for afbureaukratisering og vedligeholdelse af det offentliges brug af åbne standarder. I forhold til *DS 484* er *ISO*-standarden mere fleksibel og appellerer både til større og mindre organisationer.

Det er op til de enkelte myndigheder, hvorvidt de allerede nu vil skifte standard, eller om de vil vente, til næste revision af *ISO*/IEC 27001 er gennemført, hvilket formodes at være i 2013. Udgivelsen af den nye standard efterfølges af en overgangsperiode, hvor institutionerne har tid til at skifte til den nye standard.

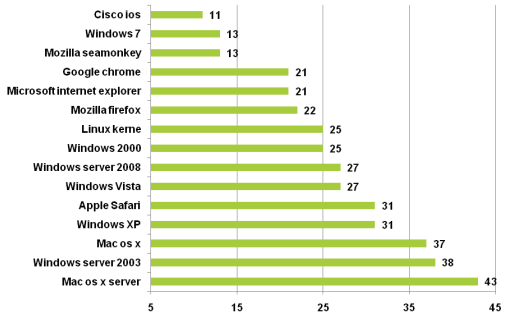
3.3. Microsoft vs Waledac

Microsoft fik den 22. februar 2010 nedlagt fogedforbud mod en række domæner, som folkene bag botnettet Waledac anvendte til at styre det med. Dermed fik bagmændene vanskeligere ved at sende kommandoer til de pc'er, der indgik i *botnettet*.

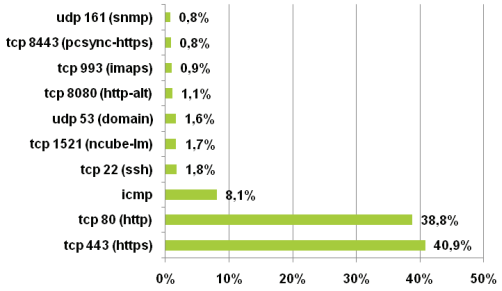
Endvidere har Microsoft i samarbejde med tyske og østrigske forskere overtaget



Figur 9. Offentliggjorte CVE-nummererede websårbarheder pr. kvartal.



Figur 10. CVE-nummererede sårbarheder offentliggjort i første kvartal 2010.



Figur 11. CVE-nummererede sårbarheder konstateret ved scanning i første kvartal 2010.

kontrollen med 60.000 pc'er i *botnettet*, som nu modtager kommandoer fra servere, som ikke styres af bagmændene. Der har efterfølgende været uenighed om effekten af lukningen.

3.4. GovCert til mere end staten

Den statslige varslingstjeneste for internettrusler, GovCERT, har som led i UMTS-aftalen fra november 2009 fået udvidet sin kundekreds.

Efter en del kritik offentliggjorde IT- og Telestyrelsen på et informationsmøde den 8. marts 2010, at GovCert, der forventes fuldt operationsdygtig i løbet af 2010, også skal have informations- og varslingsaktiviteter rettet mod kommuner, regioner og visse kritiske sektorer. Ud over at alle offentlige institutioner nu kan benytte GovCERT, vil det således også være muligt for telesektoren, elforsyningssektoren og finanssektoren at benytte tjenesten.

Desuden vil GovCERT i samarbejde med DK•CERT gennemføre en varslings- og informationsindsats rettet mod borgere samt små og mellemstore virksomheder i et såkaldt nationalt CERT-samarbejde.

3.5. Phishing mod PBS

Den 7. marts 2010 udsendte PBS igen en advarsel om, at deres navn og tjenester blev misbrugt til målrettet indsamling af kreditkortinformationer fra danskere. Mailen var som ved tilsvarende angreb et halvt år tidligere øjensynligt afsendt af PBS og skrevet på fejlfrit dansk. Men den var falsk og stammede fra svindlere, der benytter *phishing* til at opsamle fortrolige oplysninger.

Ifølge sikkerhedsfirmaet CSIS, der analyserede *phishing*-angrebet, var bagmændene de samme, som tidligere har udført identiske angreb med misbrug af PBS' og Danske Banks varemærker. Mailen kan således være et led i det samme angreb.

Hvad er ISO/IEC 27001?

ISO/IEC 27001 er en normativ standard – det vil sige, at den stiller krav – i en serie af standarder kaldet 27000-familien af standarder. Den anden normative standard er ISO/IEC 27006. I familien indgår der udover de to normative standarder en række standarder med retningslinjer for, hvordan en organisation kan implementere og overholde de normative standarder.

IT- og Telestyrelsen[8]

PBS phishing-mail

Fra: PBS Kortsystemer <pbs@pbs.dk>
Dato: 7. mar. 2010 05.10
Emne: Meddelelse om begrænset kontoadgang (PBS Kortsystemer)
Til:

Som et led i vores sikkerhedsforanstaltninger gennemgår vi jævnligt aktivitet i PBS-systemet. Under en nylig gennemgang har vi opdaget et problem med din konto.

For at kunne imødekomme bestemmelserne i den finansielle servicebranche, har vi brug for flere oplysninger til at bekræfte din identitet. Download og udfyld formularen.

Venlig hilsen

PBS Compliance-afdelingen

PBS.dk[10]

8 *IT- og Telestyrelsen, 2010; "Fra DS 484 til ISO 27001".*

9 *PBS.dk, 2010; "PBS' navn misbrugt i forsøg på phishing".*

4. Ordliste

Botnet: Et *botnet* er et netværk af computere, som en angriber kan fjernstyre fra centralt hold. Navnet kommer af "robot" og "net". Ejerne af computerne ved ikke, at deres pc er inficeret med et *botnet*-program og indgår i *botnettet*. Angriberen udnytter gerne sine "robotter" til udsendelse at foretage koordinerede denial of service-angreb eller udsende spam- og *phishing*-mails

Brute-force: Dækker i datalogien over en udtømmende afsøgning af et løsningsrum. Inden for it-sikkerheden betegner det afprøvningen af kombinationer af brugernavne og kodeord fra foruddefinerede lister.

Cross-site request forgery (CSRF): En metode, der muliggør at uautoriserede parametre og kommandoer eksekveres på serveren gennem henvendelser fra en bruger som websitet har tillid til. Metoden kan fx medføre overtagelse af brugerens session til det enkelte site.

Cross-site scripting (XSS): En metode, hvor adressen på et sårbart website udnyttes til at vise yderlig information eller afvikle programmer. Der er forskellige former for *cross-site scripting*, som gør det muligt at udføre komplekse angreb. Metoden kan fx anvendes til *phishing*, hvor brugeren bliver omdirigeret til et forfalsket website. En angriber kan udnytte et website, som en bruger har tillid til, til at få adgang til fortrolig information.

CVE, CVE-nummer: Common Vulnerabilities and Exposures, forkortet CVE, er en liste over offentligt kendte *sårbarheder* i software. Listen dækker *sårbarheder* i de fleste kendte og alment udbredte programmer, men ikke i skræddersyet eller internt udviklet software, der ikke er i distribution, såsom de fleste webapplikationer.

DS 484: Dansk standard for varetagelse af it-sikkerhed.

Fast flux: Teknologi, der hurtigt og løbende skifter den netværks- eller IP-adresse, der er tilknyttet et givent domæne. Bruges fx til *phishing*-sider for at forhindre, at de bliver sporet og lukket ned. Teknologien så dagens lys i 2007, blandt andet i forbindelse med Storm-*ormen*.

Forskningsnettet: Et højhastighedsnetværk, der forbinder danske universiteter og forskningsinstitutioner. Ud over det fysiske netværk forsyner *Forskningsnettet* brugerne med en række tjenester til forskning, samarbejde og kommunikation.

ISO 27001: Risikobaseret international standard for varetagelse af it-sikkerhed.

Malware, skadelig kode: Sammentrækning af malicious software eller på dansk ondsindet kode. *Malware* er en samlebetegnelse for vira, *orme*, *trojanske heste*, keyloggere, spyware, adware, *botnet*-programmer og lignende.

Orm: Et program, der spreder sig i netværk ved at udnytte *sårbarheder* i dets com-

putere. I TCP/IP-verdenen sker det typisk ved, at *orm*eprogrammet kontakter den port, som det sårbare program lytter på.

Phishing: Svindelmetode, der går ud på at narre fortrolige oplysninger fra ofrene. Forsøg på *phishing* optræder ofte i e-mails, der henviser til websider. Websiden angiver at tilhøre offerets bank eller kreditkortselskab eller lignende, men er i virkeligheden under svindlernes kontrol.

Portscanning: Kortlægning af åbne porte på internettet, der har til formål at identificere sårbare services knyttet til dem. En *portscanning* foregår typisk ved, at der forespørges efter mange porte på få maskiner, eller én port på mange maskiner. Oftest benyttes et program til at foretage portscanninger. Brugen af firewalls vil som udgangspunkt lukke for adgangen til maskinens åbne porte.

Sårbarhed: En fejl i et it-system, som en angriber kan udnytte til at få adgang til systemet, forhindre det i at fungere eller på anden måde misbruge det.

Sårbarhedsscanning: Kortlægning af kendte *sårbarheder* knyttet til services på et systems åbne porte. Benyttes ofte efter foregående *portscanning*.

Trojansk hest: Et program der har andre, ofte ondartede, funktioner end dem som det foregiver at have. *Trojanske heste* indeholder ofte dialer-, bagdørs- eller keylogger-funktionalitet, eller benyttes til installation af *virus*, *botnet*-programmer og lignende. *Trojanske heste* identificeres ofte af anti*virus*- og antispyware-programmer.

Virus: Et program, der inficerer andre programfiler. Når den inficerede programfil køres, aktiveres *virussen*, og den inficerer andre programfiler. Oprindelig kunne kun egentlige programmer indeholde *virus*, men dokumenter med makroer kan nu også gøre det. *Virus* spredes ofte som mail vedlagt en *trojansk hest*, der indeholder *virussen* selv.

5. Figuroversigt

6. Referencer

F-Secure.com, 2009; "*F-Secure security lab - virus world map*"; www.f-secure.com/en_EMEA/security/worldmap/

Gartner, 2008; "*Why malware filtering Is necessary in the web gateway*"; www.gartner.com/DisplayDocument?doc_cd=158459

Havard.edu, 2009; "*The economics of online crime*"; people.seas.harvard.edu/~tmoore/jep09.pdf

IT- og Telestyrelsen, 2010; "*Fra DS 484 til ISO 27001*"; shttp://www.itst.dk/sikkerhed/standarder/iso-27001/iso-27001/fra-ds-484-til-iso-27001

Ministeriet for Videnskab, Teknologi og Udvikling, 2009; "*Sander: Styrket dansk bekæmpelse af internettrusler*"; vtu.dk/nyheder/pressemeddelelser/2009/styrket-dansk-bekaempelse-af-internettrusler/

MessageLabs Intelligence, 2009; "*Messagelabs intelligence Q3/september 2009*"; www.messagelabs.com/mlireport/MLI_2009.09_Sept_SHSFINAL_EN.pdf

nvd.nist.gov; "*CVE and CCE statistics query page*"; web.nvd.nist.gov/view/vuln/statistics

PBS.dk, 2010; "*PBS' navn misbrugt i forsøg på phishing*"; http://www.pbs.dk/da/temaer/nyheder/Pages/PBS-navnmisbrugtiforsoegpaaphishing.aspx

Sans.org, 2009; "*The top cyber security risks*"; www.sans.org/top-cyber-security-risks/#trends

Wikipedia.org, 2009; "*Malware*"; da.wikipedia.org/wiki/Malware

Kontakt:

DK•CERT, UNI•C
Centrifugevej, Bygn. 356
Kgs. Lyngby 2800

Tel. +45 3587 8887
URL: https://www.cert.dk
Email: cert@cert.dk